أنواع الجرائم الإلكترونية و إجراءات مكافحتها

اعداد :

سـوريـــة ديـــش

– باحث دكتوراه جامعة جيلالي ليابس سيدي بلعباس الجزائر

ملخص :

إن التقدم التكنولوجي، وتكنولوجيا المعلومات و الاتصالات أصبحت تأخذ حيزا مهما في التعاملات اليومية، وأصبح الكمبيوتر هو محور كل التعاملات بالنسبة للأشخاص، المؤسسات، الشركات و مختلف الإدارات. اتسعت في الآونة الأخيرة دائرة استخدام الشبكات الإلكترونية للمعلومات، كوسيلة اتصال دولية في شتى مجالات الحياة، لتحقيق ما تصبو إليه الإنسانية من السرعة في إنجاز المشاريع، اختصار الوقت والمسافات وحتى الجهد البدني والذهني. وأضحت هذه الشبكات تحوي معلومات غير محصورة في مجال محدد، بل تتعلق بكافة ميادين الحياة الاجتماعية، الاقتصادية، العلمية وغيرها.

إلا أن الاستخدام المتزايد لهذه الأنظمة المعلوماتية أدى إلى الكثير من المخاطر و أفرز أنواعا من الجرائم ، أصبح بما يعرف الجرائم الالكترونية. و تنوعت هذه الجرائم المعلوماتية من تزوير سرقة معلومات و أموال – اختراق لنظم – جرائم ماسة بالأخلاق و الآداب العامة.... ، و ذلك عن طريق الدخول غير المشروع إلى جهاز حاسب آلي أو نظام معلوماتي أو شبكة معلوماتية ، بغرض تدمير ، تغيير أو إعادة نشر بيانات أو معلومات سرية أو شخصية ، إتلاف مستندات أو موقع أو نظام الكتروني و ما شابه ، ناهيك عما تسببه من خلافات بين الأفراد بسبب التشهير أو إشاعة الأخبار الكاذبة ، التهديد، الابتزاز لشخص طبيعي أو معنوي.

كلمات مفتاحية :تكنولوجيا – الجرائم الإلكترونية – شبكة – المعلوماتية – اتصال

The types of electronic crime and action against

Abstract:

The technological progress and information and communications technology has become taking occupy an important place in the daily trading, and computer is becoming the focus of all dealings for person, institutions, companies, and various departments.

Have expanded use of electronic networks of information as a means of an international contacts to achieve what they legitimately aspire to humanity from the speed in the completion of the projects , shortening the time and the distances, and includes many information but the increasing use has led to many risks and the types of electronic crimes.

Varied electronic crimes between fraud, information theft and the money, through illegal entry to the computer or an information system for the purpose of destroying or change or redeployment of personal information, damaging documents .

In addition to disagreements between individuals for spreading false news , threats , extortion and defamation.

Keywords : technology – electronic crimes – information network

مـقـدمــة:

فلقد ظهر حديثا نمط جديد من الجرائم ، نظرا للتحولات الاقتصادية ، الاجتماعية و الثقافية ...، تجسد في الجرائم المعلوماتية التي أصبحت تمثل خطرا كبيرا على الأفراد و المؤسسات وبياناتهم و ارتكاب جرائم بوسائل الكترونية.

حيث تعاني المجتمعات الإلكترونية في الآونة الأخيرة من انتهاك للحقوق والخصوصيات الالكترونية و ذلك في ظل انتشار الجريمة الالكترونية، و جاء تطور هذا النوع من الجرائم بالتزامن مع التطورات التي تطرأ على التقنيات والتكنولوجيا، الأمر الذي دفع الدول إلى العمل الجدي للحد من هذه الجرائم التي تلحق الضرر بالأفراد من خلال التوعية والوسائل الوقائيّة الأمنية وغيرها من الطرق. **تُعرف الجرائم الالكترونية** بأنها تلك الأفعال الإجرامية الناتجة من خلال أو بواسطة استخدام المعلوماتية و التقنية الحديثة المتمثلة في الكمبيوتر و المعالجة الآلية للبيانات ، أو بنقلها[1].

و لقد عرفته منظمة التعاون الاقتصادي و التنمية" OECD : كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية و المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية[2] ."

و لقد نص المشرع الجزائري على هذه الجرائم في قانون 09-04 و اصطلح على تسميته : " الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال " و عرفها بأنها " : جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أية جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية[3] . "

إن جرائم الكمبيوتر في نطاق الظاهرة الإجرامية المستحدثة، جرائم تنصب على معطيات الحاسوب (بيانات و معلومات و برامج) و تطال الحق في المعلومات ، ويستخدم لاقترافها وسائل تقنية تقتضي استخدام الحاسوب بوصفه نظاما حقق التزاوج بين تقنيات الحوسبة و الاتصالات.

و تتم **من خلال الاتصال بالإنترنت و يكون هدفها اختراق الشبكات أو تخريبها أو التحريف أو التزوير أو السرقة و الاختلاس أو قرصنة، جرائم أخلاقية، ابتزاز، تشهير و سرقة حقوق الملكية الفكرية.** و لقد جرم المشرع الجزائري الأفعال الماسة بنظام المعالجة الآلية للمعطيات ، و سميت بالغش المعلوماتي في القسم السابع مكرر من قانون العقوبات[4].

الإشكالية :

فنظرا لانتشار الجريمة الالكترونية بما يهدد الفرد و المجتمع في اقتصاده ، سيادته و أمنه الوطني و التأثيرات السلبية لهذه الأنواع من الجرائم نطرح التساؤلات التالية:

- ماهي أنواع هذه الجرائم ؟
- ماهي الخطوات الهامة للقضاء على جرائم تقنية المعلومات من خلال استخدام الوسائل الإلكترونية درءا للتجاوزات من قوانين و إجراءات ؟

أهداف الدراسة:

تتلخص أهداف الدراسة إلى توضيح:

- التمكن من الوصول إلى شبكة الانترنيت لسرقة المعلومات.
- التشهير و الابتزاز و التهديد لهدف شخصي أو مادي أو بدافع الانتقام.
- الكسب الغير الشرعي للمال عن طريق اختراق للمواقع الالكترونية ، أو الوصول إلى تقنية المعلومات و إعادة بيعها.

- أنواع السرقة أهمها سرقة بطاقات الائتمان و حسابات الأفراد و المؤسسات المالية.
- توضيح وضع التشريعات السارية في الجزائر فيما يخص الجرائم الإلكترونية.

أهمية الدراسة:

لا يخفى على أحد مدى أهمية الموضوع من حيث ظهور الحاجة الملحة لدراسة الموضوع نظرا:

- للتطور الحاصل في مجال استعمال شبكات الانترنيت، التعاقد الإلكتروني، شبكات التواصل الاجتماعي وغيرها.
- التطور التقني والتكنولوجي في مجال الثورة التكنولوجية و الاتصالات و ما نجم عنه من قرصنة، توفر برمجيات نسخ المعلومات المخزنة، التجسس و غيرها من الأعمال الغير المشروعة.
- حاجة الأفراد إلى الحماية في مجال المعاملات الالكترونية، لحماية أملاكه المالية والمعنوية وحماية أسراره الخاصة

منهجية البحث:

ولمعالجة الموضوع اعتمدنا المنهج الوصفي لإبراز وتحديد أنواع الجرائم الإلكترونية وطنيا ، إلى جانب المنهج التحليلي لتقييم الأساليب القانونية و التقنية في القضاء و مكافحة جرائم المعلوماتية .

تحليل النتائج و الاستنتاجات :

- مكافحة الجرائم الإلكترونية يتطلب رسم سياسة وطنية و دولية تفرض عقوبات صارمة على مرتكبي جرائم الإنترنت.
- يستلزم أيضا أساليب و تقنيات متطورة لحماية المعلوماتية و التمكن من الكشف عن مرتكبي هذه الأعمال الغير مشروعة.

المبحث الأول أنواع الجرائم الإلكترونية:

إن أنواع الجرائم الالكترونية كثيرة حيث لم يوضع لها معايير محددة من أجل تصنيفها و هذا راجع إلى التطور المستمر للشبكة و الخدمات التي تقدمها.

وقد تضاربت الآراء لتحديد أنواع جرائم الانترنت وتعددت التصنيفات، فهناك من عددها بحسب موضوع الجريمة ، وأخر قسمها بحسب طريقة ارتكابها.

و قد صنفها معهد العدالة القومي بالولايات المتحدة الأمريكية عام 1985 بحسب علاقتها بالجرائم التقليدية.

الصنف الأول يتمثل في الجرائم المنصوص عليها في قانون العقوبات متى ارتكبت باستعمال الشبكة.

الصنف الثاني تضمن دعم الأنشطة الإجرامية ويتعلق الأمر بما تلعبه الشبكة من دور في دعم جرائم غسيل الأموال، المخدرات الاتجار بالأسلحة، واستعمال الشبكة كسوق للترويج غير المشروع في هذه المجالات.

الصنف الثالث بجرائم الدخول في نظام المعالجة الآلية للمعطيات، وتقع على البيانات والمعلومات المكونة للحاسوب وتغييرها أو تعديلها أو حذفها مما يغير مجرى عمل الحاسوب.

الصنف الرابع فتضمن جرائم الاتصال وتشمل كل ما يرتبط بشبكات الهاتف، و ما يمكن أن يقع عليها من انتهاكات باستغلال ثغرات شبكة الإنترنت.

وأخيرا صنف الجرائم المتعلقة **بالاعتداء على حقوق الملكية الفكرية** ويتمثل في عمليات نسخ البرامج دون وجه حق، وسرقة حقوق الملكية الفكرية المعروضة على الشبكة دون إذن من صاحبها بطبعها وتسويقها واستغلالها بأي صورة طبقا لقانون حماية الملكية الفكرية**[5]** . إن تقسيم الجرائم الإلكترونية بما أنها ترتكب باستخدام

الحاسوب كأداة أساسية، فدور الحاسوب في تلك الجرائم يكون هدفا للجريمة أو أداة لها . [6]

المطلب الأول الجرائم المعلوماتية الواقعة بواسطة النظام المعلوماتي:

و هنا لا يكون النظام المعلوماتي هو محل الجريمة ، بل يكون الحاسب الآلي هو الوسيلة لتسهيل النتيجة الإجرامية باستخدام النظام المعلوماتي، و يكون الهدف من ورائها الربح بطريق غير مشروع، الإعتداء على أموال الغير ، الإعتداء على الأشخاص و سلامتهم و حياتهم الخاصة ، أو في سمعتهم و شرفهم و الإعتداء على أمن الدولة و أسرارها.

الفرع الأول : الجرائم الواقعة على الأشخاص

فرغم الإيجابيات و الفوائد التي جاءت بها الشبكة المعلوماتية و التسهيلات المقدمة للفرد ، إلا أنها جعلته أكثر عرضة للانتهاك ، و منها:

- **جريمة التهديد** :وهو الوعيد يقصد به زرع الخوف في النفس، بالضغط على إرادة الإنسان ، وتخويفه من اضرار ما ستلحقه أو ستلحق أشخاص له بها صلة، ويجب أن يكون التهديد على قدر من الجسامة المتمثلة بالوعيد بإلحاق الأذى ضد نفس المجني عليه أو ماله أو ضد نفس او مال الغير ، ولا يشترط أن يتم إلحاق الأذى فعلا أي تنفيذ الوعيد ،لأنها تشكل جريمة أخرى قائمة بذاتها ، تخرج من إطار التهديد الى التنفيذ الفعلي ، وقد يكون التهديد مصحوبا بالأمر أو طلب لقيام بفعل أو الامتناع عن الفعل ، أو لمجرد الانتقام ، و لقد أصبحت الانترنت الوسيلة لارتكاب جرائم التهديد ، والتي في حد ذاتها تحتوي عدة وسائل لإيصال التهديد للمجني عليه لما تتضمنه من نوافذ وجدت للمعرفة كالبريد الإلكتروني أو الويب...
- **انتحال شخصية** : و هو استخدام شخصية فرد للاستفادة من ماله أو سمعته أو مكانته، و لقد تميزت بسرعة الانتشار خاصة في الأوساط التجارية . و تتم

بجمع قدر كبير من المعلومات الشخصية المراد انتحال شخصيته ، للإستفادة منها لارتكاب جرائمه عن طريق استدراج الشخص ليدلي بمعلوماته الشخصية الكاملة ، كالإسم، العنوان الشخصي،رقم بطاقة الإئتمان للتمكن من الوصول لماله أو سمعته... عن طريق الغش.

- **انتحال شخصية أحد المواقع :** و يتم ذلك عن طريق اختراق أحد المواقع للسيطرة عليه، ليقوم بتركيب برنامج خاص به هناك، باسم الموقع المشهور . [7]
- **جرائم السب و القذف :**للمساس بشرف الغير و سمعتهم، و اعتبارهم، و يكون القذف و السب كتابيا،أو عن طريق المطبوعات أو رسوم، عبر البريد الإلكتروني أو الصوتي، صفحات الويب، بعبارات تمس الشرف.

فيقوم المجرم بنشر معلومات تكون مغلوطة عن الضحية ، و قد يكون شخصا طبيعيا أو معنويا ، لتصل المعلومات المراد نشرها إلى أعداد كبيرة من مستخدمي شبكة الانترنيت.

- **المواقع الإباحية و الدعارة :** وجود مواقع على شبكة الانترنيت تحرض على ممارسة الجنس للكبار و القصّر ، و ذلك بنشر صور جنسية للتحريض على ممارسة المحرمات ، و الجرائم المخلة بالحياء عن طريق صور ، أفلام ، رسائل... بالإضافة إلى **انتشار الصور و مقاطع الفيديو المخلة بالآداب على مواقع الانترنت من قبل الغزو الفكري لكي يتداولها الشباب و إفساد أفكارهم وإضعاف إيمانهم.**
- **و توفر الشبكة تسهيلا للدعارة، عبر آلاف المواقع الإباحية، و تسوق الدعارة و تستثمر لها مبالغ ضخمة مع استخدام أحدث التقنيات.**
- **التشهير وتشويه السمعة** :يقوم المجرم بنشر معلومات قد تكون سرية أو مضللة أو مغلوطة عن ضحيته، والذي قد يكون فرداً أو مؤسسة تجارية أو سياسية، تتعدد الوسائل المستخدمة في هذا النوع من الجرائم، لكن في مقدمة

هذه الوسائل إنشاء موقع على الشبكة يحوي المعلومات المطلوب نشرها أو إرسال هذه المعلومات عبر القوائم البريدية إلى أعداد كبيرة من المستخدمين، و يُضم لهذه الجرائم كذلك تشويه السمعة، الشائعات و الأخبار الكاذبة لمحاربة الرموز السياسية و الفكرية و حتى الدينية من أجل تشكيك الناس في مصداقية هؤلاء الأفراد، و قد يكون الهدف من ذلك هو الابتزاز.

كل هذه الجرائم الماسة بالأشخاص تدخل ضمن الحياة الخاصة للأفراد التي كفلها القانون و في مقدمته الدستور الجزائري حيث تنص المادة 40 منه " : تضمن الدولة عدم انتهاك حرمة الإنسان [8] ." و عليه يمكن استخدام الشبكة المعلوماتية في الاعتداء على حرمة الفرد و حياته الخاصة و حرمته ، و الحريات العامة للأفراد ، و هو مخالف للقانون و معاقب عليه.

الفرع الثاني : الجرائم الواقعة على الأموال

أصبحت المعاملات الشراء، البيع و الإيجار تتم عبر الشبكة المعلوماتية، و ما انجرّ عليه من وسائل الدفع و الوفاء ، فابتكرت معه طرق و وسائل للسطو على هذا التداول المالي بطريق غير مشروع ، كالتحويل الإلكتروني ، السرقة ، القرصنة و غيرها.

- **السرقة الواقعة على البنوك :** يتم سرقة المال بالطرق المعلوماتية عن طريق اختلاس البيانات و المعلومات الشخصية للمجني عليهم ، و الاستخدام لشخصية الضحية ليقوم بعملية السرقة المتخفية ، ما يؤدي بالبنك إلى التحويل البنكي للأموال الالكتروني أو المادي إلى الجاني. حيث يستخدم الجاني الحاسب الآلي لدخول شبكة الانترنيت و الوصول إلى المصارف و البنوك ، و تحويل الأموال الخاصة بالعملات إلى حسابات أخرى[9] . **وعملية السرقة الإلكترونية كالاستيلاء على ماكينات الصرف الآلي والبنوك ، يتم فيها نسخ البيانات الإلكترونية لبطاقة الصراف الآلي ومن ثم استخدامها لصرف أموال من حساب الضحية ، أو إنشاء صفحة انترنت مماثلة جدا لموقع احد البنوك**

الكبرى أو المؤسسات المالية الضخمة لتطلب من العميل إدخال بياناته أو تحديث معلوماته بقصد الحصول على بياناته المصرفية وسرقتها. رسائل البريد الواردة من مصادر مجهولة التي توهم صاحب البريد الإلكتروني بفوزه بإحدى الجوائز أو اليانصيب وتطالبه بموافاة الجهة برقم حسابه المصرفي، و الأمثلة كثيرة...

- **تجارة المخدرات عبر الأنترنيت :** تتعلق بالترويج للمخدرات و بيعها، و التحريض على استخدامها ، و صناعتها بمختلف أنواعها.
- **غسيل الأموال :** تمارس عبر الأنترنيت ، حيث استفاد الجناة ما وصلت إليه عصر التقنية المعلوماتية لتوسيع نشاطهم الغير مشروع في غسيل أموالهم ، بتوفير السرعة ، و تفادي الحدود الجغرافية، و القوانين المعيقة لغسيل الأموال ، و كذا لتشفير عملياتهم و سهولة نقل الأموال و استثمارها لإعطائها الصبغة الشرعية[10] .
- **الاستعمال الغير الشرعي للبطاقات الائتمانية :** رافق استخدام البطاقات الائتمانية ، الاستيلاء عليها باعتبارها نقود الكترونية و ضلك إما بسرقة أرقام البطاقات ثم بيع المعلومات للآخرين ، من خلال الحصول على كلمة السر المدرجة في ملفات أنظمة الحاسب الآلي للضحية عن طريق الاحتيال ، و ذلك بايهامه بحصول ربح ، فيقدم الضحية معلومات تمكن الجاني من التصرف في ماله ،[11] أو إساءة استخدام الغير البطاقات الإئتمانية، كأن يقوم السارق استعمال البطاقة للحصول على السلع و الخدمات أو سحب مبالغ مالية بموجبها من أجهزة التوزيع الآلي أو السحب باستخدام بطاقات مزورة[12] .
- **الجرائم الواقعة على حقوق الملكية الفكرية و الأدبية :** كذلك يكون النظام المعلوماتي وسيلة للاعتداء على حقوق الملكية الفكرية ، و ذلك بالسطو على المعلومات التي يتضمنها نظام معلوماتي آخر، و تخزين و استخدام هذه المعلومات دون إذن صاحبها، حيث يعد اعتداء على الحقوق المعنوية و على قيمتها المادية[13] .

- **قرصنة البرمجيات :هي عملية نسخ أو تقليد لبرامج إحدى الشركات العالمية على اسطوانات وبيعها للناس بسعر أقل، و جريمة نسخ المؤلفات العلمية و الأدبية بالطرق الالكترونية المستحدثة** .حيث أن المعلومة الأدبية و الفكرية ذات قيمة أدبية و مادية بالإضافة إلى براءات الاختراع التي تخول لمالكها حق معنوي و آخر مالي.
- نص عليها المشرع في الدستور في المادة 44 : " حقوق المؤلف يحميها القانون [14] ." بالإضافة إلى قوانين المتعلقة بحقوق المؤلف و الحقوق المجاورة ، و براءات الاختراع[15].

الفرع الثالث : الجرائم الواقعة على أمن الدولة

تقع هذه الجرائم باستعمال النظام المعلوماتي سواء للإفشاء الأسرار التي تخص مصالح الدولة و نظام الدفاع الوطني، أو الإرهاب ، التجسس ..نصت عليها المادة 394 مكرر 2 : " تضاعف العقوبة المنصوص عليها في هذا القسم اذا استهدفت الجريمة الدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام دون الاخلال بتطبيق عقوبات أشد[16] ."

- **الإرهاب : تستخدم المجموعات الإرهابية حالياً تقنية المعلومات لتسهيل الأشكال النمطية من الأعمال الإجرامية. وهم لا يتوانون عن استخدام الوسائل المتقدمة مثل: الاتصالات والتنسيق، وبث الأخبار المغلوطة، وتوظيف بعض صغار السن، وتحويل بعض الأموال في سبيل تحقيق أهدافهم .**
- **و يقوم الإرهابيون باستخدام الإنترنت لاستغلال المؤيدين لأفكارهم وجمع الأموال لتمويل برامجهم الإرهابية ، والاستيلاء على المواقع الحساسة وسرقة المعلومات وامتلاك القدرة على نشر الفيروسات، و ذلك يرجع إلى العدد المتزايد من برامج الكمبيوتر القوية والسهلة الاستخدام والتي يمكن تحميلها مجانا** .

- **التجسس :** يقوم المجرمون بالتجسس على الدول و المنظمات و الشخصيات و المؤسسات الوطنية أو الدولية ، و تستهدف بخاصة : التجسس العسكري ، السياسي، و الاقتصادي ، و ذلك باستخدام التقنية المعلوماتية، و تمارس من قبل دولة على دولة ، أو من شركة على شركة ... و ذلك بالإطلاع على المعلومات الخاصة المؤمنة في جهاز آلي ، و غير مسموح بالإطلاع عليها، كأن تكون من قبيل أسرار الدولة.

المطلب الثاني : الجرائم المعلوماتية الواقعة على النظام المعلوماتي و هي الجرائم الواقعة على النظام المعلوماتي التي قد تستهدف سواء المكونات المادية لنظام \المعلومات أو برامج النظام المعلوماتي، أو المعلومات المدرجة بالنظام المعلوماتي على النحو التالي:

الفرع الأول : الجرائم الواقعة على المكونات المادية للنظام المعلوماتي

و يقصد به الأجهزة و المعدات الملحقة به و التي تستخدم في تشغيله كالأسطوانات ، الكابلات... و الاعتداء عليها يكون بالسرقة لهذه المعدات ، أو عن طريق الإتلاف العمدي كاحراقها، ضرب الآلات بشيء ثقيل، العبث بمفاتيح التشغيل خربشة الأسطوانات لكي لا تصبح صالحة للاستعمال[17] .

الفرع الثاني : الاعتداء على برامج النظام المعلوماتي

و يتوجب هنا معرفة و دراية ذات درجة عالية في مجال البرمجة، و تقع هذه الجرائم إما على البرامج التطبيقية أو برامج التشغيل.

- **البرامج التطبيقية** :و هنا يقوم الجاني بتحديد البرنامج ثم التلاعب فيه للإستفادة منه ماديا، و ذلك ب**تعديل البرنامج :** و يكون الهدف من تعديل البرامج اختلاس النقود ،حتى و لو كان باستقطاع مبالغ قليلة لكن لفترات زمنية طويلة لتحقيق الفائدة ، بدون إثارة الشبهات.

- أما **التلاعب:** فيأخذ عدة أشكال ، فقد يكون عن طريق زرع برنامج فرعي في البرنامج الأصلي مثلا يسمح له الدخول غير المشروع في العناصر الضرورية للنظام المعلوماتي، حيث يصعب اكتشاف هذا البرنامج لدقته و صغر حجمه[18].
- **برامج التشغيل: و هي** البرامج المسؤولة عن عمل نظام معلوماتي من حيث قيامها بتنظيم و ضبط ترتيب التعليمات الخاصة بالنظام.
- و تقوم الجريمة هنا عن طريق تزويد البرنامج بمجموعة تعليمات إضافية ليسهل الوصول إليها بواسطة شفرة تسمح الحصول على جميع المعطيات التي يتضمنها النظام المعلوماتي[19] . و تأخذ شكلين هما **المصيدة** :و هو إعداد برنامج به ممرات و فراغات في البرنامج و تفرعات إضافية، وهنا يمكن للمبرمج استخدام البرنامج في أي وقت ، و يصبح المهيمن على النظام و على صاحب العمل .
- أما **تصميم برنامج:** هو قيام برنامج خصيصا يصعب اكتشافه لارتكاب الجريمة و مراقبة تنفيذها.

الفرع الثالث : الجرائم الواقعة على المعلومات المدرجة بالنظام المعلوماتي

إن المعلومات المعالجة آليا هي أساس عمل النظام المعلوماتي ، لأنها ذات قيمة مادية و اقتصادية، لذلك تعد هدفا للجرائم الإلكترونية من خلال التلاعب فيها او إتلافها.

- يكون **التلاعب** في المعلومات الموجودة على النظام المعلوماتي بطريقة مباشرة أو غير مباشرة، فيتم **التلاعب المباشر** عن طريق إدخال معلومات بمعرفة المسؤول عن القسم المعلوماتي، كضم مستخدمين غير موجودين بالعمل بهدف الحصول على مرتباتهم، الإبقاء على مستخدمين تركوا العمل للحصول على مبالغ شهرية، أو عن طريق تحويل لمبالغ وهمية لدى العاملين بالبنوك باستخدام النظام المعلوماتي بالبنك، و تسجيلها و إعادة ترحيلها و إرسالها لحساب آخر في بنك آخر، بهدف اختلاس الأموال[20] . أما **التلاعب الغير**

مباشر ، فيتم عن طريق التدخل لدى المعلومات المسجلة بالنظام المعلوماتي باستخدام أحد وسائط التخزين، أو التلاعب عن بعد بمعرفة أرقام و شفرات الحسابات ،[21] قصد التلاعب في الشرائط الممغنطة ، أو باستخدام الجاني كلمة السر أو مفتاح الشفرة ، و امكانية تسلل الجاني إلى المعلومات المخزنة و الحصول عللى المنفعة المالية من مسافات بعيدة.

- **إتلاف المعلومات** في مجال المعلوماتية بالاعتداء على الوظائف الطبيعية للحاسب الآلي ، و ذلك بالتعدي على البرامج و البيانات المخزنة و المتبادلة بين الحواسب و شبكاته، و تدخل ضمن الجرائم الماسة بسلامة المعطيات المخزنة ضمن النظام المعلوماتي، و يكون الاتلاف العمدي للبرامج و البيانات كمحوها أو تدميرها الكترونيا ، أو تشويهها على نحو يجعلها غير صالحة للاستعمال.

و إن من خصائص استخدام النظام المعلوماتي في طبيعتها المتعدية للحدود ، و طابعها التقني الذي يعقد إثباته من حيث التقنيات التكنولوجية الحديثة.

المبحث الثاني: إجراءات مكافحة الجريمة

واكب المشرع الجزائري بقدر قليل الحركة التشريعية لمكافحة الجرائم الالكترونية لكنها اصطدمت بعدة صعوبات نظرا لخصوصية الجريمة من جهة ، و سرعة تطورها من جهة أخرى.

المطلب الأول : القوانين لمكافحة الجريمة

باعتبار الفقه الراجح بأن برامج الحاسوب مالا كون المعلومات تعتبر شيئا منقولا مملوكا للغير ، فهي صالحة لأن تكون محل سرقة التي تتحقق يتحويل ما يحتويه القرص من معلومات إلى سند آخر ، و **الاختلاس** هنا يطبق بشأنه المادة 350 من قانون العقوبات[22] . بما في ذلك سرقة المعلومات ، ذلك لأنه لا تحدد طبيعة الشيء محل الجريمة مادية أو معنوية ، زيادة على أن الأشياء المعنوية لها قيمة اقتصادية.

و عليه يطبق القاضي الجزائي أحكام السرقة على أموال الإعلام الآلي.

أما وقوع البرامج و البيانات تحت طائلة **النصب** و الاحتيال باعتبارها أموالا و منقولات ، تطبق بشأنها المادة 372 من ق.ع[23] .

ثم إن الجريمة المعلوماتية لها طابع غير مادي للقيم، إلا أن بعض القيم مثل البرامج و المعطيات تصلح أن تكون محلا لخيانة الأمانة بصفتها بضائع ، تطبق بشأنها المادة 376 من ق.ع بتهمة **خيانة الأمانة**[24] . و لما كانت المعلومات و البرامج من قبيل الأموال فهي مشمولة بالحماية الجزائية، فإذا كانت محل إتلاف أو تدمير ، و نتج عنها خسائر ، فيمكن إخضاع الجريمة لنص المادة 412 من ق.ع[25] . المحددة للأشياء الخاضعة **للإتلاف**.

و إن المشرع الجزائرى قد جرم الأفعال الماسة بنظام المعالجة الالية للمعطيات أو ما سميت بالغش المعلوماتي ، بموجب القسم السابع مكرر من قانون العقوبات ، [26] فقد عاقب بالحبس من ثلاثة اشهر إلى سنة و بغرامة من 50.000 إلى 100.000 دج ، في حالة إدخال ، بطريق الغش معطيات فين المعالجة أو نفس العقوبة على المحاولة [27] . و تضاعف العقوبة اذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة[28] .

أما إذا ترتب عنها تخريب نظام اشتغال المنظومة تكون العقوبة من 6 اشهر الى سنتين حبس و الغرامة من 50.000 إلى 150.000 دج[29] . و تعاقب المادة 394 مكرر1 على المساس بمنظومة معلوماتية بالإدخال، الإزالة او التعديل بطريق الغش ، بالحبس من 6 اشهر إلى 3 سنوات و بغرامة من 500.000إلى 2.000.000 دج[30] .

في حين نصت المادة 394 مكرر2 على عقوبة الحبس من شهرين إلى 3 سنوات و بغرامة من 1.000.000 الى 5.000.000 دج لكل من يقوم عمدا و بطريق الغش بتصميم او بحث او تجميع أو توفير ،نشر ،الاتجار في معطيات مخزنة او معالجة او

مرسلة عن طريق منظومة معلوماتية ، و إفشاء او نشر المعطيات [31] . و قد عاقب المشرع الجزائري الشخص المعنوى بموجب المادة 394 مكرر 4 بغرامة تعادل خمس مرات الحد الاقصى للغرامة المقررة للشخص الطبيعي عند ارتكابه للأفعال المجرمة بهذا القانون[32] .

و قد تضمنت المادة 394 مكرر3 مضاعفة العقوبة المقررة لجرائم الغش المعلوماتي، اذا استهدفت الجريمة الدفاع الوطني او الهيئات و المؤسسات الخاضعة للقانون العام . [33]و يعاقب المشرع على الاتفاق بين الأطراف أو المشاركة في الجرائم المعلوماتية ، إذا ما جسدت بأفعال مادية[34] .

و أقر بمصادرة الاجهزة و البرامج و الوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من جرائم الغش المعلوماتي ،علاوة على إغلاق المحل إذا كانت الجريمة قد ارتكبت بعلم مالكها [35] .كما يعاقب على الشروع بذات العقوبة[36] .

و عليه فإن بالإضافة إلى النص صراحة على جرائم المعلوماتية ، فإنه يمكن أن تكون بعض الجرائم الأخرى الغير المذكورة ضمن هذا القسم محلا لجرائم الأموال و النصب و التزوير ... يمكن استنتاجه و القياس عليه ، رغم اختلاف الفقهاء ، و إن كان من الأفضل أن ينص المشرع صراحة بالنصوص القانونية على اعتبار المعلومات و المعطيات و البرامج في النظام المعلوماتي أحد عناصر الذمة المالية و يحدد العقوبات الواجبة لها، نظرا للحاجة الملحة لحماية برامج الحاسب الآلي في الوسط القانوني من جهة حماية لحقوق الغير من جهة أخرى ، حيث لا يمكن تكييف جريمة لم ينص عليها القانون صراحة في القانون الجنائي على أي عمل و لو كان غير مشروع مما يساعد على تهرب المجرمين عن أفعالهم بحجة حماية الحقوق المكفولة دستوريا[37] .

فالإشكالات التي تثيرها هذا النوع من الجرائم نظرا لحداثته نجد:

- حداثة القوانين المنظمة لها.

- التزايد الكمي في أعداد الجرائم الإلكترونية.
- التطور النوعي في أساليب ارتكابها.
- عدم مواكبة التشريعات للمجتمع الرقمي الذي هو في تطور مستمر.
- صعوبة الوصول إلى شهود للجريمة.
- صعوبة إثباتها خاصة فيما يخص الركن المادي الذي يتطلب نصوص قانونية خاصة بها ، خاصة في ظل شرعية العقوبات ، حيث " لا جريمة و لا عقوبة أو تدابير أمن بغير قانون[38] ."
- وجود مبدأ تنازع القوانين خاصة في ظل وجود مبدأ إقليمية القوانين ، لأن في غالبيتها جرائم عابرة للحدود، و منه أيضا صعوبة الملاحقة الأمنية في حال اشتراك عناصر إجرامية داخل و خارج الوطن.
- صعوبة الكشف عن الشروع في الجرائم الإلكترونية.

المطلب الثاني : الطرق الكفيلة للحد من جرائم الإلكترونية

و لمكافحة الجريمة يجب رسم سياسات دولية تفرض عقوبات صارمة على مرتكبي جرائم الإنترنت، إذ يستلزم التدخل الوطني و الدولي نظراً للخطورة الجسيمة للأمر.

و كذلك الاعتماد على أساليب وتقنيات متطورة للتمكن من الكشف عن هوية مرتكب الجريمة والاستدلال.

كما يجب توعية الأفراد ونصحهم لماهية الجرائم الالكترونية و كل ما يترتب عليها من مخاطر و الحرص على الحفاظ على سرية المعلومات الخاصة بالعناوين الإلكترونية كالحسابات البنكية، والبطاقات الائتمانيّة وغيرها ،و تسليط الضوء على موضوع الجرائم المتصلة بالكمبيوتر و سبل مكافحتها، للحيلولة دون المزيد من انتشارها.

عدم الكشف عن كلمة السر نهائيا وتغييرها بشكل مستمر، مع تجنب تخزين الصور الخاصة بالأفراد على مواقع التواصل الاجتماعي وأجهزة الحاسوب.

تجنب تحميل أي برنامج مجهول المصدر و استمرارية تحديث برامج الحماية الخاصة بأجهزة الحاسوب.

و لا بد من التحسيس و التوعية و التعريف للعامة ، و نشر المعرفة عبر الإعلام حول هذه الجرائم و خصائصها و نشر الوعي حول خطورتها، و آليات مكافحتها.

و يجب إنشاء خطوط هاتفية للمواطنين تسمح لهم الإبلاغ عن هذه الجرائم حين اكتشافها إلى السلطات المعنية.

- و يبقى توضيح أهمية تطوير التشريعات الموجودة بما يواكب التطور التكنولوجي و ضرورة تنظيم الجرائم المستحدثة ، ضرورة حتمية لسد النقص في قانون العقوبات ، من حيث الصور الأخرى من الجرائم التي لم يتم تنظيمها في قوانيننا الجزائرية، و الإجراءات الجزائية ، بما يتناسب مع خصوصية إجراءات الضبط ، إجراءات التحقيق، و تكييف الأفعال المرتكبة وطنيا ، و التعاون الدولي في مكافحة الجرائم المعلوماتية في ظل اتفاقيات دولية ، مع تسليط الضوء على التجارب الدولية في مكافحتها للجرائم الالكترونية.

خاتمة:

إن الجرائم الالكترونية ظاهرة بالغة الخطورة ، و إن احتمال تعرض الأشخاص أو المؤسسات لجريمة إلكترونية صارت مرتفعة جدا ، ذلك أن حجم الجريمة الالكترونية في تزايد مستمر، و عمق تأثيرها السلبي على المجتمع في تزايد مستمر هو الآخر.

و لقد أثارت هذه الجرائم تساؤلات كثيرة ، نظرا لجسامة أخطارها و خسائرها الفادحة و سرعة انتشارها ، حيث أصبح التعامل مع صور هذه الجرائم موضع اهتمام الجميع، و الاحساس بأن الكل معني بشكل أو بآخر بأخطار و عواقب الجرائم الإلكترونية.

فرغم وجود هذه النصوص القانونية ، فإنها لم تضع حد للأفعال المجرمة ، لأسباب ترجع تارة أن رجال العدالة لم يتعودوا بعد على تطبيق مثل هذه النصوص، و أن

النصوص القانونية في حد ذاتها لا تلم بجميع الجرائم الالكترونية. بالإضافة إلى ندرة القضايا المعروضة قضائيا في هذا المجال سواء بسبب استغلال الفراغ القانوني في هذا المجال ، أو بما أن الجريمة هي تقنية محضة فيمكن تجاوزها تقنيا أيضا بدون ترك دليل مادي يثبتها.

فـــــالجريمة الإلكترونية تتمثل في كل سلوك غير قانوني من خلال استخدام الأجهزة الإلكترونية ، ينتج منه حصول المجرم على فوائد مادية أو معنوية .وأخيرا لا يمكن أن تكون تلك الجرائم بمنأى عن العقاب ولابد أن يكون لدينا أجهزة تتعقب مثل تلك الجرائم وتكافحها بشكل لا تتعدى به على حرية الأشخاص ولكنها أيضا لابد أن تكون على علم وبصيرة بكل ما يحدث ويشكل جرائم سواء جرائم جنائية أو جرائم تمس أمن الدولة ، وأمن الدولة بمعناها العام والواسع والذى يؤثر فى الأفكار لدى الشباب أو نشر الأفكار الخاطئة أو حتى يهز الثقة بين الفرد وحكومته.

و عليه فصدور قوانين خاصة بالجرائم الإلكترونية و الردع القانوني و من أهم الحلول لمواجهة الظاهرة ذلك أنه ما تم خلقه تقنيا يمكن تجاوزه تقنيا أيضا، فيبقى الجزاء القانوني هو الحل الوحيد للقضاء على هذه الظاهرة التي استفحلت بشكل ملحوظ.

قائمة المراجع :

- أحمد خليفة الملط ، الجرائم المعلوماتية، دار اللفكر الجامعي، القاهرة ، الطبعة الثانية 2006.
- ذكي ذكي أمين حسونة، جرائم الكمبيوتر و الجرائم الأخرى في مجال التكنيك المعلوماتي، المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، أيام 25-28 أكتوبر 1993.
- صالحة العمري، جريمة غسيل الأموال و طرق مكافحتها، مجلة الإجتهاد القضائي، العدد الخامس، مخبر أثر الإجتهاد القضائي على حركة التشريع، جامعة محمد خيضر، بسكرة، د.س.ن.
- صغير يوسف، الجريمة المرتكبة عبر الأنترنيت ، *مذكرة ماجستير* في قانون الأعمال، كلية الحقوق و العلوم السياسية، جامعة مولود معمري ، تيزي وزو، 2013.
- عباس أبو شامة ، التعريف بالظواهر الإجرامية المستحدثة: حجمها، أبعادها، و نشاطها في الدول العربية، الندوة العلمية للظواهر الإجرامية المستحدثة و سبل مواجهتها، تونس ، أيام 29-30 جوان 1999.
- عبد العال الدريبي، الجريمة الالكترونية بين التشريع و القضاء في الدول الغربية، المركز العربي لأبحاث القضاء الالكتروني بتاريخ 01 مارس 2013.
- محمد الشوا، ثورة المعلومات و انعكاساتها على قانون العقوبات، الطبعة الثانية، دار النهضة العربية، القاهرة، 1994.
- محمد بن عبد الله بن علي المنشاوي، جرائم الانترنيت في المجتمع السعودي، ماجستير في العلوم الشرطية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2003.
- Le rapport du conseil du l'Europe, 15,18 novembre 1976.

- Voir l'information nouvelle, mai 1976, N° 73.
- **النصوص القانونية :**
- دستور الجمهورية الجزائرية الديمقراطية الشعبية 1996 ، ج.ر رقم 76 المؤرخة في 8 ديسمبر 1996، المعدل و المتمم بالقانون رقم 16-01 المؤرخ في 6 مارس 2016، ج.ر رقم 14 المؤرخة في 7 مارس 2016 .
- الأمر 66-156، المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات ، المعدل و المتمم.
- الأمر 03-05 المؤرخ في 19 جويلية 2003، المتعلق بحقوق المؤلف و الحقوق المجاورة،
- الأمر 03-07 المؤرخ في 19 جويلية 2003 ، المتعلق ببراءات الإختراع.
- القانون 09-04 ، المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها .

[1] محمد الشوا، ثورة المعلومات و انعكاساتها على قانون العقوبات، الطبعة الثانية، دار النهضة العربية، القاهرة، 1994 ،ص7.

[2] أحمد خليفة الملط ، الجرائم المعلوماتية، دار الفكر الجامعي، القاهرة ، الطبعة الثانية 2006، ص 87.

[3] ينظر المادة 2-أ من القانون 09-04 ، المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، ج.ر المؤرخة في 16 أوت 2009، العدد 47.

[4] ينظر القسم السابع مكرر ، المواد من 394 مكرر إلى 349 مكرر 7 من الأمر 66-156المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات، المعدل و المتمم.

[5] عبد العال الدريبي، الجريمة الالكترونية بين التشريع و القضاء في الدول الغربية، المركز العربي لأبحاث القضاء ألالكتروني بتاريخ 01 مارس 2013.

[6] عبد العال الدريبي،المرجع السابق.

[7] محمد بن عبد الله بن علي المنشاوي، جرائم الأنترنيت في المجتمع السعودي، ماجستير في العلوم الشرطية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2003، ص 55.

[8] ينظر المادة 1/40 من دستور 1996، ج.ر رقم 76 المؤرخة في 8 ديسمبر 1996، المعدل و المتمم بالقانون رقم 16-01 المؤرخ في 6 مارس 2016، ج.ر رقم 14 المؤرخة في 7 مارس 2016.

[9] عباس أبو شامة ، التعريف بالظواهر الإجرامية المستحدثة: حجمها، أبعادها، و نشاطها في الدول العربية، الندوة العلمية للظواهر الإجرامية المستحدثة و سبل مواجهتها، تونس ، أيام 29-30 جوان 1999، ص 20.

[10] صالحة العمري، جريمة غسيل الأموال و طرق مكافحتها، مجلة الإجتهاد القضائي، العدد الخامس، مخبر أثر الإجتهاد القضائي على حركة التشريع، جامعة محمد خيضر، بسكرة، د.س.ن ، ص 179.

[11] صغير يوسف، الجريمة المرتكبة عبر الأنترنيت ، مذكرة ماجستير في قانون الأعمال، كلية الحقوق و العلوم السياسية، جامعة مولود معمري ، تيزي وزو، 2013، ص 45.

[12] أحمد خليفة الملط، المرجع السابق، ص 196.

[13] أحمد خليفة الملط، المرجع السابق، ص 184.

[14] ينظر المادة 2/44 من الدستور ، المرجع السابق.

[15] ينظر الأمر 03-05 المؤرخ في 19 جويلية 2003، المتعلق بحقوق المؤلف و الحقوق المجاورة، و كذلك الأمر 03-07 المؤرخ في 19 جويلية 2003 ، المتعلق ببراءات الإختراع، ج.ر رقم 44 المؤرخة في 23 جويلية 2003.

[16] ينظر المادة 394 مكرر2 من الأمر 66-156، المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات ، المعدل و المتمم.

[17] ذكي ذكي أمين حسونة، جرائم الكمبيوتر و الجرائم الأخرى في مجال التكنيك المعلوماتي، المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، أيام 25-28 أكتوبر 1993، ص 471.

[18] Le rapport du conseil du l'Europe , 15,18 novembre 1976.

[19] أحمد خليفة الملط ، المرجع السابق،ص175.

[20] محمد سامي الشوا، المرجع السابق، ص 82.

[21] Voir l'information nouvelle, mai 1976,, N° 73.

[22] ينظر المادة 350 من قانون العقوبات ، المرجع السابق.

[23] ينظر المادة 372 من قانون العقوبات ، المرجع السابق.

[24] ينظر المادة 376 من قانون العقوبات ، المرجع السابق.

[25] ينظر المادة 412 من قانون العقوبات ، المرجع السابق.

[26] ينظر المواد من 394 مكرر إلى 394 مكرر7 المعدلة بالقانون 06-23 المؤرخ في 20 ديسمبر 2006، المرجع السابق.

[27] المادة 394 مكرر.

[28] المادة 394 مكرر /2.

[29] المادة 394 مكرر /3.

[30] المادة 394 مكرر1.

[31] المادة 394 مكرر 2.

[32] المادة 394 مكرر 4.

[33] المادة 394 مكرر3.

[34] المادة 394 مكرر 5.

[35] المادة 394 مكرر6.

[36] المادة 394 مكرر7.

[37] حيث ينص الدستور في المادة 58 منه : " لا إدانة إلا بمقتضى قانون صادر قبل ارتكاب الفعل المجرم."

[38] ينظر المادة الأولى من قانون العقوبات ، المرجع السابق.